LISTING OF THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

1. (Currently Amended) A method of creating a role certificate by a user, comprising:

transmitting a role approval form, filled out and digitally signed by the user using a personal digital signature, to at least one personal role approval, wherein the user is a member of a group authorized to utilize the role certificate as a group stamp and for encryption of information which may be decrypted by a plurality of group members;

signing digitally the role approval form by the personal role approval using a personal digital signature;

creating a role certificate upon receipt of the role approval form signed by the user and the personal role approval;

notifying the user of the availability of the role certificate; and

transmitting the role certificate to the user.

2. (Currently Amended) The method recited in claim 1, wherein the role certificate comprises a public key, a private key, [[of]]a signature algorithm ID, a validity period, extensions, and at least one policy.

3. (Original) The method recited in claim 2, wherein the policy indicates all permitted uses and limitations on the role certificate.

4. (Currently Amended) The method recited in claim 3, further comprising:

identifying all members of a group as role members that will access and use ~~of~~ the role certificate;

storing the names and identifications of all role members; and

transmitting copies of the role certificate to all role members.

5. (Original) The method recited in claim 4, further comprising:

transmitting the public key portion of the role certificate to a plurality of entities outside the group; and

decrypting messages from the plurality of entities outside the group encrypted using the public key portion of the role certificate.

6. (Original) The method recited in claim 4, further comprising:

signing electronic forms by a group member utilizing the role certificate; and

transmitting electronic forms to entities outside the group.

7. (Currently Amended) A method of using a role certificate as an organizational stamp and for organizational encryption by a plurality of role members of a group, comprising:

filling out an electronic form by a role member of the plurality of role members of the group, wherein the role member is a member of a group authorized to utilize the role certificate as a group stamp and for encryption of information which may be decrypted by a plurality of group members;

signing digitally the electronic form by the role member using the role certificate;

signing digitally the electronic form by the role member using a personal signature certificate; and

transmitting the electronic form to an entity.

8. (Original) The method recited in claim 7, further comprising:

retrieving a policy associated with the role certificate by the entity; and

determining if the role certificate signature supplied is valid as a signature for the electronic form.

9. (Currently Amended) The method recited in claim 7, further comprising:

transmitting a public key portion of the role certificate by the role member to the entity;

encrypting information by the entity;

transmitting the information to ~~the role member~~any of the plurality of role members of the group; and

decrypting the information by any ~~member~~of the plurality of role members of the group having the ~~digital~~role certificate.

10. (Currently Amended) The method recited in claim 9, wherein the role certificate comprises a public key, a private key, [[of]]a signature algorithm ID, a validity period, extensions, and at least one policy, wherein the extensions indicate that the role certificate may be used for both encryption and as a digital signature.

11. (Original) A method of replacing an expiring role certificate, comprising:

displaying a list of roles to a user who is either a role member or a role administrator; wherein the user is a member of a group authorized to utilize the role certificate as a group stamp and for encryption of information which may be decrypted by a plurality of group members;

selecting a role which is about to expire for renewal by the user;

determining if the user is authorized to renew the role based upon verification of the user's personal digital signature;

generating a new role certificate having a private and public key; and

transmitting the new role certificate to the user.

12. (Original) The method recited in claim 11, the transmitting of the new role certificate to the user is done over an encrypted secure communications line.

13. (Currently Amended) The method recited in claim 11, wherein prior to the transmitting of the new role certificate to the user, the new role certificate is transmitted to a certificate

authority for approval, and the new role certificate is not transmitted to the user without the approval.

14. (Original) The method recited in claim 13, wherein the public key portion of the role certificate is stored on a server for access by individuals and entities outside of the group.

15. (Currently Amended) The method recited in claim 14, wherein the ~~the~~ private key portion of the role certificate is stored in a key recovery authority for recovery in case of loss or expiration.

16. (Currently Amended) The method recited in claim 11, wherein the role certificate comprises a public key, a private key, [[of]]a signature algorithm ID, a validity period, extensions, and at least one policy.

17. (Currently Amended) A method of revoking a role certificate used as an organizational stamp and for organizational encryption by authorized members of the organization, comprising:

transmitting a signature certificate to a registration web server by a user, wherein the user is a member of a group authorized to utilize the role certificate as a group stamp and for encryption of information which may be decrypted by a plurality of group members;

authenticating by accessing a directory that the user is still a member of the organization;

listing roles of which the user is a role member or a role authority; and

removing the role certificate associated with the role from a directory database.

18. (Original) The method recited in claim 17, wherein when the role certificate is removed from the directory database the role associated with the role certificate remains intact on the database.

19. (Original) The method recited in claim 18, further comprising:

generating a new role certificate for the role when the role certificate is removed from the directory database;

establishing a secure encrypted communications line with the user; and

transmitting the role certificate to the user.

20. (Original) The method recited in claim 19, further comprising:

notifying all role members associated with the role of the removal of the role certificate and the creation of the new role certificate when the new role certificate is created.

21. (Currently Amended) The method recited in claim 17, wherein the role certificate comprises a public key, a private key, [[of]]a signature algorithm ID, a validity period, extensions, and at least one policy.

22. (Original) A method of recovery of an expired role certificate associated with the role used for organizational encryption and as an organizational stamp, comprising:

transmitting a request to recover the expired role certificate along with a digital signature from a role member, wherein a role member is an entity having a right to digitally sign organizational documents using the role certificate and decrypting information sent to members of the organization which has been encrypted using the role certificate;

listing all roles that the role member is listed as a role member on;

selecting the expired role certificate from the list of roles by the role member for recovery;

contacting a key recovery authority for a copy of the role certificate; and

transmitting the role certificate to the role member.

23. (Original) The method recited in claim 22, further comprising:

authenticating that the role member is either a member of the role or a role authority for the role prior to contacting the key recovery authority.

24. (Currently Amended) The method recited in claim 22, wherein the role certificate comprises a public key, a private key, [[of]]a signature algorithm ID, a validity period, extensions, and at least one policy.

25. (Original) The method recited in claim 23, wherein all members of the role are informed of the recovery of the role certificate.

26. (Currently Amended) A method of revoking a role certificate and an associated role by a role administrator, comprising:

transmitting a request to revoke the role certificate of a role member and the associated role by the role administrator for the role certificate along with a signature certificate for the role administrator, wherein the role member is a member of a group authorized to utilize the role certificate as a group stamp and for encryption of information which may be decrypted by a plurality of group members;

searching a database for all role certificates in which the role administrator is listed as a role administrator;

displaying to the role administrator all role certificates discovered;

selecting a role certificate by the role administrator to be removed; and

deleting both the role certificate and the role from the database.

27. (Original) The method recited in claim 26, wherein a policy is deleted from a directory when the role certificate and a role are deleted from the database.

28. (Currently Amended) The method recited in claim 27, wherein the role certificate comprises a public key, a private key, [[of]]a signature algorithm ID, a validity period, extensions, and at least one policy.

29. (Currently Amended) A method of recovering a former role and an associated role certificate by a role administrator, comprising:

identifying a role certificate to be recovered;

searching a database to determine if any role members associated with the role certificate are still in the organization, wherein each of the role members are members of a group authorized to utilize the role certificate as a group stamp and for encryption of information which may be decrypted by a plurality of group members;

transmitting to at least one recovery agent a request for approval for the recovering of the role certificate when no role members are discovered to be in the organization;

receiving approval from the at least one recovery agent for recovery of the role certificate;

transmitting to the at least one recovery agent the role certificate retrieved when the ~~recover~~ recovery agent supplies an approval to recover the role certificate; and

transmitting the role certificate to the role administrator by the recovery agent.

30. (Original) The method recited in claim 29, wherein the at least one recovery agent is at least two recovery agents and both recovery agents must approve recovery before recovery of the role certificate occurs.

31. (Currently Amended) The method recited in claim 30, wherein both recovery agents must be authenticated as having authority to authorize the recovery of the role certificate prior to the role certificate being sent to the recovery agent.

32. (Currently Amended) A computer program embodied on a computer readable medium and executable by a computer to create a role certificate for a user, comprising:

transmitting a role approval form filled out and digitally signed by the user using a personal digital signature to at least one personal role approval, wherein the user is a member of

a group authorized to utilize the role certificate as a group stamp and for encryption of information which may be decrypted by a plurality of group members;

signing digitally the role approval form by the personal role approval using a personal digital signature;

creating a role certificate upon receipt of the role approval form signed by the user and all personal role approval;

notifying the user of the availability of the role certificate; and

transmitting the role certificate to the user.

33. (Currently Amended) The computer program recited in claim 32, wherein the role certificate comprises a public key, a private key, [[of]]a signature algorithm ID, a validity period, extensions, and at least one policy.

34. (Original) The computer program recited in claim 33, wherein the policy indicates all permitted uses and limitations on the role certificate.

35. (Currently Amended) The computer program recited in claim 34, further comprising:

identifying all members of a group as role members that will access and use ~~of~~ the role certificate;

storing the names and identifications of all role members; and

transmitting copies of the role certificate to all role members.

36. (Original) The computer program recited in claim 35, further comprising:

transmitting the public key portion of the role certificate to a plurality of entities outside the group; and

decrypting messages from the plurality of entities outside the group encrypted using the public key portion of the role certificate.

37. (Original) The computer program recited in claim 35, further comprising:

signing electronic forms by a group member utilizing the role certificate; and

transmitting electronic forms to entities outside the group.

38. (Currently Amended) A computer program embodied on a computer readable medium and executable by a computer for using a role certificate as an organizational stamp and for organizational encryption by a plurality of role members of a group, comprising:

filling out an electronic form by a role member of the plurality of role members of the group, wherein the role member is a member of a group authorized to utilize the role certificate as a group stamp and for encryption of information which may be decrypted by a plurality of group members;

signing digitally the electronic form by the role member using the role certificate;

signing digitally the electronic form by the role member using a personal signature certificate; and

transmitting the electronic form to an entity.

39. (Original) The computer program recited in claim 38, further comprising:

retrieving a policy associated with the role certificate by the entity; and

determining if the role certificate signature supplied is valid as a signature for the electronic form.

40. (Currently Amended) The computer program recited in claim 38, further comprising:

transmitting a public key portion of the role certificate by the role member to the entity;

encrypting information by the entity;

transmitting the information to ~~the role member~~any of the plurality of role members of the group; and

decrypting the information by any ~~member~~of the plurality of role members of the group having the ~~digital~~role certificate.

41. (Currently Amended) The computer program recited in claim 40, wherein the role certificate comprises a public key, a private key, [[of]]a signature algorithm ID, a validity period, extensions, and at least one policy, wherein the extensions indicate that the role certificate may be used for both encryption and as a digital signature.

42. (Currently Amended) A computer program embodied on a computer readable medium and executable by a computer for replacing an expiring role certificate, comprising:

displaying a list of roles to a user who is either a role member ~~of~~ or a role administrator ~~for~~, wherein the user is a member of a group authorized to utilize the role certificate as a group stamp and for encryption of information which may be decrypted by a plurality of group members;

selecting a role which is about to expire for renewal by the user;

~~and~~ determining if the user is authorized to renew the role based upon verification of the user's personal digital signature;

generating a new role certificate having a private and public key; and

transmitting the new role certificate to the user.

43. (Original) The computer program recited in claim 42, the transmitting of the new role certificate to the user is done over an encrypted secure communications line.

44. (Currently Amended) The computer program recited in claim 42, wherein prior to the transmitting of the new role certificate to the user, the new role certificate is transmitted to a certificate authority for approval, and the new role certificate is not transmitted to the user without the approval.

45. (Original) The computer program recited in claim 44, wherein the public key portion of the role certificate is stored on a server for access by individuals and entities outside of the group.

46. (Currently Amended) The computer program recited in claim 45, wherein the ~~the~~ private key portion of the role certificate is stored in a key recovery authority for recovery in case of loss or expiration.

47. (Currently Amended) The computer program recited in claim 46, wherein the role certificate comprises a public key, a private key, [[of]]a signature algorithm ID, a validity period, extensions, and at least one policy.

48. (Currently Amended) A computer program embodied on a computer readable medium and executable by a computer for revoking a role certificate used as an organizational stamp and for organizational encryption by authorized members of the organization, comprising;

transmitting a signature certificate to a registration web server by a user, wherein the user is a member of a group authorized to utilize the role certificate as a group stamp and for encryption of information which may be decrypted by a plurality of group members;

authenticating by accessing a directory that the user is still a member of the organization;

listing roles of which the user is a role member or a role authority; and

removing the role certificate associated with the role from a directory database.

49. (Original) The computer program recited in claim 48, wherein when the role certificate is removed from the directory database the role associated with the role certificate remains intact on the database.

50. (Currently Amended) The computer program recited in claim 49 ~~deaths~~, further comprising:

generating a new role certificate for the role when the role certificate is removed from the directory database;

establishing a secure encrypted communications line with the user; and

transmitting the role certificate to the user.

51. (Original) The computer program recited in claim 50, further comprising:

notifying all role members associated with the role of the removal of the role certificate and the creation of the new role certificate when the new role certificate is created.

52. (Currently Amended) The computer program recited in claim 49, wherein the role certificate comprises a public key, a private key, a signature algorithm ID, a validity period, extensions, and at least one policy.

53. (Original) A computer program embodied on the computer readable medium and executable by computer for recovery of an expired role certificate associated with the role used for organizational encryption and as an organizational stamp, comprising:

transmitting a request to recover the expired role certificate along with a digital signature from a role member, wherein a role member is an entity having a right to digitally signed organizational documents using the role certificate and decrypting information sent to members of the organization which have been encrypted using the role certificate;

listing all roles that the role member is listed as a role member on;

selecting the expired role certificate from the list of roles by the role member for recovery;

contacting a key recovery authority for a copy of the role certificate; and

transmitting the role certificate to the role user.

54. (Original) The computer program recited in claim 53, further comprising:

authenticating that the role member is either a member of the role or a role authority for the role prior to contacting the key recovery authority.

55. (Currently Amended) The computer program recited in claim 53, wherein the role certificate comprises a public key, a private key, [[of]]a signature algorithm ID, a validity period, extensions, and at least one policy.

56. (Original) The computer program recited in claim 54, wherein all members of the role are informed of the recovery of the role certificate.

57. (Currently Amended) A computer program embodied on a computer readable medium and executable by a computer for revoking a role certificate and an associated role by a role administrator, comprising:

transmitting a request to revoke the role certificate of a role member and the associated role by the role administrator for the role certificate along with a signature certificate for the role administrator, wherein the user is a member of a group authorized to utilize the role certificate as a group stamp and for encryption of information which may be decrypted by a plurality of group members;

searching a database for all role certificates in which the role administrator is listed as a role administrator;

displaying to the role administrator all role certificate discovered;

selecting a role certificate by the role administrator to be removed; and

deleting both the role certificate and the role from the database.

58. (Original) The computer program recited in claim 57, wherein a policy is deleted from a directory when the role certificate and a role are deleted from the database.

59. (Currently Amended) The computer program recited in claim 58, wherein the role certificate comprises a public key, a private key, [[of]]a signature algorithm ID, a validity period, extensions, and at least one policy.

60. (Currently Amended) A computer program embodied on a computer readable medium and executable by a computer for recovering a former role and an associated role certificate by a role administrator, comprising:

identifying a role certificate to be recovered;

searching a database to determine if any role members associated with the role certificate are still with the organization, wherein the each of the role members are members of a group authorized to utilize the role certificate as a group stamp and for encryption of information which may be decrypted by a plurality of group members;

transmitting to at least one recovery agent a request for approval for the recovering of the role certificate;

receiving approval from the at least one recovery agent for recovery of the role certificate;

transmitting to the at least one recovery agent the role certificate retrieved; and

transmitting the role certificate to the role administrator by the recovery agent.

61. (Original) The computer program recited in claim 60, wherein the at least one recovery agent is at least two recovery agents and both recovery agents must approve recovery before recovery of the role certificate occurs.

62. (Currently Amended) The computer program recited in claim [[31]]61, wherein both recovery agents must be authenticated as having authority to authorize the recovery of the role certificate prior to the role certificate being sent to the recovery agent.

63. (Currently Amended) A role certificate for organizational encryption and for use as [[a]]an organizational stamp or seal, comprising:

a public key to be transmitted to entities outside the organization to use as an encryption key;

a private key to decrypt information encrypted using the public key;

a signature algorithm ID to be used in generating a digital signature with the role certificate;

a validity period indicating when the role certificate will expire;

extensions having a plurality of bits which designate characteristics associated with the role certificate, wherein when a bit for encryption is ~~sent~~set and a bit for signature is set, the role certificate may be used for both digital signatures and encryption; and

a policy defining the limitations on valid usage of the role certificate.

64. (Currently Amended) The ~~computer program~~ role certificate recited in claim [[62]]63, wherein the role certificate may be used by any member authorized within the organization for decrypting encrypted information and signing on behalf of the organization.

65. (Currently Amended) The ~~computer program~~ role certificate recited in claim [[62]]63, wherein the role certificate is created by a role authority and deleted by the member of the organization designated as a role member for the role certificate, wherein an associated role for the role certificate may not be deleted by the role member.

66. (Currently Amended) The ~~computer program~~ role certificate recited in claim 64, wherein any time ~~where~~ that the role certificate is used to sign on behalf of the organization, a signature certificate for the entity signing must be included.